KILLTEST

20% de descuento en todos los productos

Preguntas del examen

020-100

Security Essentials - Exam 020, version 1.0

1.Which of the following methods can be used to ensure integrity of data during transmission?
A. Passwords
B. Encryption
C. Two-factor authentication
D. Redundancy
Answer: B

2.Which of the following backup types is best suited for daily use?
A. Synthetic backup
B. Full backup
C. Incremental backup
D. Differential backup
Answer: C

3.Which of the following is a security implication of physical access to a computer?
A. Unauthorized access to data
B. Improved processor performance
C. Decreased memory capacity
D. Increased network speed
Answer: A

4.You want to access a website that is blocked in your country.
Which of the following solutions would be the most appropriate for accessing the website?
A. Network-attached storage
B. Using an unencrypted public Wi-Fi network
C. A public VPN provider
D. Clearing your browser's cache
Answer: C

5.You are setting up a Bluetooth connection between your smartphone and a wireless speaker.
What security measure should you take to protect your data?
A. Use a strong and unique password for the Bluetooth connection
B. Enable Bluetooth pairing mode on your smartphone
C. Leave the Bluetooth connection open to all nearby devices
D. Disable Bluetooth after the connection is established
Answer: A

6.What is the primary function of an endpoint firewall?
A. To protect a single device from unauthorized access or attacks
B. To store data securely
C. To manage hardware components
D. To improve network performance
Answer: A

7.What is the darknet?
A. A type of network that is used for illegal activities
B. A type of network that is only accessible through TOR
C. A type of network that is not connected to the internet
D. Cloud Storage
Answer: B

8.Which of the following legal concepts is concerned with compensating someone for harm caused by a security breach?
A. Public law
B. Copyright law
C. Financial compensation claims
D. Liability
Answer: D

9.What is the purpose of the GDPR?
A. To encourage the collection and sharing of personal data without restriction
B. To encourage the use of insecure data storage methods
C. The GDPR is a type of virus that infects computer systems and steals personal information
D. To protect personal information of individuals in the European Union
Answer: D

10.Which of the following is a type of software that is embedded in hardware devices and provides instructions to the hardware to perform specific tasks?
A. Desktop applications
B. Server software
C. Firmware
D. Web applications
Answer: C

11.What is blockchain?
A. Blockchain is a digital currency.
B. Blockchain is a type of database management system
C. Blockchain is a proprietary software platform developed by a single company.
D. A type of database that uses a network of nodes to store information in a decentralized manner
Answer: D

12.Which of the following is a fraudulent activity designed to deceive individuals into providing sensitive information or transferring funds to unauthorized parties in the context of IT security?
A. Intrusion detection system
B. Data encryption
C. Firewall
D. Scamming
Answer: D

13.What is the purpose of an RFID tag?
A. To enable wireless communication between devices
B. To store and transfer data wirelessly
C. To connect devices to the internet
D. To control network traffic
Answer: B

14.Which type of asymmetric encryption algorithm provides better security than an equivalent RSA key of the same size and is commonly used in mobile devices?
A. RSA
B. Diffie-Hellman
C. ECC
D. IDEA
Answer: C

15.Which of the following is a technology used for sending and receiving encrypted emails in Mozilla Thunderbird?
A. SMTP
B. OpenPGP and S/MIME
C. POP3

D. IMAP
Answer: B

16.What is the most effective type of phishing for targeting key executives within an organization?
A. Spearphishing
B. Whaling
C. Vishing
D. Smishing
Answer: B

17.You are tasked with securely storing backups of sensitive data in a cloud service. Which security measure should you implement to help ensure data privacy?
A. Physical security measures for the cloud server
B. Encryption of backups before uploading to the cloud service
C. Two-factor authentication for accessing backups
D. Password-protected backups
Answer: B

18.Which of the following is a type of attack where an attacker intercepts and reads network traffic?
A. Botnet
B. Traffic interception
C. DoS
D. Packet filter
Answer: B

19.Which of the following pertains to the possible damage resulting from mistakes and service disruptions?
A. Cost Reduction
B. Operational Risks
C. Increased Productivity
D. System Errors
Answer: B

20.Which of the following risk management strategies seeks to minimize risk to an acceptable level?
A. Risk avoidance

B. Risk transfer
C. Risk mitigation
D. Risk acceptance
Answer: C

21.You suspect that someone has been intercepting and reading the network traffic on your home WiFi network.
What type of attack is this?
A. Distributed Denial of Service (DDoS)
B. DoS
C. Traffic interception
D. Botnet
Answer: C

22.Dion Solutions, a large enterprise company, needs to deploy a new software application for their employees to use. They want to make sure that their employees have access to the latest version of the software and that it is easy to manage.
Which cloud deployment model would be the best choice for them?
A. SaaS
B. IaaS
C. PaaS
D. SECaaS
Answer: A

23.Which of the following is a key feature of BitLocker?
A. Free and open-source
B. Cross-platform support
C. Integrated with Windows
D. Encrypts only files
Answer: C

24.Which of the following threats to personal information uses stolen information to make purchases or obtain loans?
A. Identity theft
B. Cyberbullying
C. Financial fraud
D. Social engineering attack
Answer: C

25.Which of the following is an example of confidential information?
A. Publicly available information
B. Bug Bounty programs
C. Public press releases
D. Personal identification numbers (PINs)
Answer: D

26.Which of the following is true about S/MIME?
A. S/MIME provides end-to-end encryption and digital signatures for email communications.
B. S/MIME provides protection against spam.
C. S/MIME is limited to certain email clients.
D. S/MIME is a server that manages email communications.
Answer: A

27.Which of the following is the role of OpenPGP key servers?
A. OpenPGP key servers manage email communications.
B. OpenPGP key servers are only used with Mozilla Thunderbird.
C. OpenPGP key servers provide antivirus protection for email communications.
D. They allow users to store and retrieve public keys associated with an email address.
Answer: D

28.Which of the following is a plain text protocol?
A. SSL
B. HTTP
C. TLS
D. HTTPS
Answer: B

29.Which of the following devices is an example of an IoT device?
A. Router
B. Smartphone
C. Desktop computer
D. Printer
Answer: B

30.Which of the following is a router that is used as a gateway to forward traffic from a device to other networks?
A. Default Gateway
B. Switch
C. Modem
D. Access Point
Answer: A

31.Which term describes the ability to prove that a specific individual or entity performed an action, such as sending a message or conducting a transaction?
A. Non-repudiation
B. Confidentiality
C. Availability
D. Integrity
Answer: A

32.What is a script blocker?
A. A browser extension that prevents pop-up windows
B. A browser extension that removes or blocks advertisements
C. A browser extension that blocks scripts from running on websites
D. A browser extension that helps users control and manage cookies
Answer: C

33.You are concerned about your internet activity being tracked by your ISP. Which of the following solutions would be the most appropriate for protecting your privacy?
A. End-to-end encryption
B. TOR
C. Transfer encryption
D. Disabling your firewall
Answer: B

34.Your computer has become infected with a program that is causing it to perform slowly and display unwanted advertisements.
What type of attack is this?
A. DoS
B. Malware
C. Phishing
D. Exploit

Answer: B

35.What is Trusted Computing?
A. A protocol for secure communication between devices
B. A method for encrypting data on a physical medium
C. A security standard for IoT devices
D. A set of hardware and software technologies to enhance security
Answer: D

36.What is the primary goal of an attacker who interrupts services, such as by launching a Distributed Denial of Service (DDoS) attack?
A. To manipulate or delete data
B. To extort ransom from the targeted organization
C. To cause a disruption in the availability of the targeted system or service
D. To gain unauthorized access to the targeted system or service
Answer: C

37.Which of the following is an example of an administrative control?
A. Firewalls
B. Biometric scanners
C. Password policies
D. Intrusion detection systems
Answer: C

38.Which tool can help protect your privacy by preventing user tracking through browser fingerprinting?
A. HTTP cookies
B. User tracking software
C. Script blockers
D. Ad blockers
Answer: C

39.As the IT administrator of a company, you are responsible for implementing a cloud storage solution. You need to consider the potential issues related to the use of cloud services, especially concerning data synchronization and accessibility.
Which of the following should you be particularly aware of when deploying the cloud storage solution?
A. Data loss prevention

B. Encryption at rest
C. Data redundancy
D. Dependence on Internet connection
Answer: D

40.What is multi-factor authentication (MFA)?
A. A tool used to bypass authentication
B. A security measure that uses only one factor to authenticate a user
C. A security measure that uses multiple factors to authenticate a user
D. A tool used to securely store passwords
Answer: C

41.What is OpenPGP?
A. An email client for encryption and signing messages.
B. An open-source implementation of the S/MIME standard.
C. An open standard for email encryption and signing using public key cryptography.
D. A certificate authority (CA) for S/MIME encryption.
Answer: C

42.Which of the following terms refers to the deliberate act of accessing, manipulating, or deleting data without authorization?
A. Firewall
B. Encryption
C. Phishing
D. Hacking
Answer: D

43.What device is used to cable network jacks from a wall into a central location for termination into a single punch down block?
A. Router
B. Firewall
C. Switch
D. Patch panel
Answer: D

44.What is a common function of adware?
A. Encrypting data on a system
B. Stealing sensitive information

C. Displaying unwanted advertisements
D. Providing remote access to a system
Answer: C

45.What is single sign-on (SSO)?
A. A tool used to securely store and generate passwords
B. A tool used to create weak passwords
C. A tool used to decrypt passwords
D. A tool that allows users to log in to multiple systems with a single set of credentials
Answer: D

46.Which of the following is a common source for security incident information and guidance?
A. Computer Emergency Response Team (CERT)
B. Security incident response plan
C. Risk assessment report
D. IT forensics report
Answer: A

47.Your friend complains that they recently installed a new browser extension to help find online discounts. However, since installing it, they have been experiencing an excessive amount of pop-up ads and unrelated advertising banners on web pages. What type of malware is most likely responsible for these symptoms?
A. Trojan malware
B. Adware
C. Ransomware
D. Spyware
Answer: B

48.You work for a large company that has employees who need to access the company network from remote locations.
Which of the following solutions would be the most appropriate for providing secure remote access?
A. An organization-specific VPN
B. Setting up an open Wi-Fi network
C. Using plaintext email for communication
D. Relying on FTP for file transfers
Answer: A

49.You are using a public Wi-Fi network at a coffee shop to access sensitive information.
What security measure should you take to protect your information?
A. Use a weak password for your accounts
B. Share your login credentials with others using the same Wi-Fi network
C. Leave your computer unattended while you step away
D. Use a virtual private network (VPN) to encrypt your data
Answer: D

50.What is the purpose of The Onion Router (TOR) network?
A. Anonymity and Privacy
B. Network Monitoring
C. Data Storage
D. Speed Optimization
Answer: A

51.What is one of the primary factors that determines data retention requirements for backups?
A. The cost implications of retaining backup data for extended periods
B. The sensitivity of the data being backed up
C. The length of time an organization has been in operation
D. Regulatory requirements and compliance
Answer: D

52.What is the purpose of a Public Key Infrastructure (PKI)?
A. To manage private keys
B. To manage digital certificates and public keys
C. To manage user accounts
D. To manage encryption algorithms
Answer: B

53.Which of the following provides even stronger security through the use of Simultaneous Authentication of Equals (SAE) encryption?
A. WPA3
B. WPA2
C. WEP
D. WPA
Answer: A

54.Which of the following is a characteristic of a secure password?
A. Short length
B. No special characters
C. Complexity
D. Infrequent changes
Answer: C

55.What are some security risks associated with Smart Devices and IoT networks?
A. Overheating and battery malfunction
B. Poor internet connectivity and network lag
C. Data breaches and unauthorized access
D. Display and resolution issues
Answer: C

56.What do web browsers check when verifying the validity of an X.509 certificate?
A. subjectAltName
B. Expiration date and issuer
C. Key usage
D. Subject
Answer: B

57.You want to send a private message to a friend using an instant messaging app. Which of the following solutions would be the most appropriate for ensuring the privacy of your conversation?
A. TOR
B. A proxy server
C. Transfer encryption
D. End-to-end encryption
Answer: D

58.What potential issue can arise from using some security tools that mistakenly identify legitimate activities as malicious?
A. False positives
B. False negatives
C. Improved detection accuracy
D. Reduced system performance impact
Answer: A

59.Which of the following terms refers to a process of evaluating a system's security posture?
A. Security Audit
B. CVE
C. Security assessments
D. ISMS
Answer: C

60.Which of the following is a fraudulent Wi-Fi access point that appears to be legitimate and is used to eavesdrop on wireless communications?
A. Captive portal
B. De-authentication attack
C. Karma attack
D. Evil twin
Answer: D

61.Which of the following backup types only copies data that has changed since the last backup, regardless of which type of backup it was last performed?
A. Full backup
B. Incremental backup
C. Differential backup
D. Synthetic backup
Answer: B

62.Which of the following is a private IPv4 address?
A. 2001:0db8:85a3:0000:0000:8a2e:0370:7334
B. AC:DE:48:00:11:22
C. 172.16.0.1
D. 66.23.15.63
Answer: C

63.Which of the following is an example of a hybrid encryption scheme?
A. RSA
B. HTTPS
C. AES
D. SHA-256
Answer: B

64.Which of the following is a network of compromised devices used to perform malicious activities?
A. Man in the Middle
B. Traffic interception
C. DoS
D. Botnet
Answer: D

65.What is email spam?
A. Sensitive information sent via email
B. Unsolicited and unwanted email
C. Emails from trusted sources
D. Encrypted email
Answer: B

66.Which protocol is used to translate domain names into IP addresses?
A. DHCP
B. SMTP
C. 802.11
D. DNS
Answer: D

67.Which backup rotation scheme uses a sequence of full, differential, and incremental backups to create a backup history?
A. Tower of Hanoi
B. Grandfather-Father-Son
C. 3-2-1 Backup Rule
D. Monthly-Weekly-Daily
Answer: B

68.Which concept ensures that only the intended recipients can read a message?
A. End-to-end encryption
B. Transfer encryption
C. TOR
D. Proxy servers
Answer: A

69.Which of the following is a wired network connection commonly used for local area networks?
A. Twisted pair
B. Bluetooth
C. Fiber optic
D. Coaxial
Answer: A

70.What is the potential risk of publishing personal information online?
A. Enhanced privacy
B. Identity theft
C. Increased productivity
D. Improved mental health
Answer: B

71.Which of the following encryption methods is used for email encryption and requires the use of a public key and a private key pair?
A. Certificate Authority
B. S/MIME
C. OpenPGP
D. SMTP STARTTLS
Answer: C

72.Which of the following is used to verify the identity of a website?
A. X.509 digital certificate
B. SSL/TLS
C. Certificate Signing Request (CSR)
D. Diffie-Hellman key exchange
Answer: A

73.Which of the following is the BEST way to securely procure and install software?
A. Downloading software from an unsecured website
B. Purchasing software from an unverified vendor
C. Installing software from a USB drive
D. Installing software from an app store
Answer: D

74.Which of the following is a network address used to identify devices in layer three of the OSI model?
A. TCP port number
B. DNS address
C. MAC address
D. IP address
Answer: D

75.What is the purpose of a rootkit?
A. To increase network speed
B. To encrypt data on a system
C. To detect and remove malware
D. To provide remote access to a system
Answer: D

76.Which of the following is a characteristic of Perfect Forward Secrecy (PFS)?
A. It relies on a single long-term private key for all sessions.
B. It is not used in modern encryption protocols.
C. It generates a unique session key for each session.
D. It uses symmetric encryption for all sessions.
Answer: C

77.What is an non-disclosure agreement (NDA)?
A. An agreement to not disclose any information
B. A contract that requires sharing confidential information with others in a business relationship
C. An agreement to disclose all information
D. An agreement to disclose some information
Answer: A

78.What is a major security concern when installing mobile applications from unknown sources?
A. Malware infection
B. Incompatible hardware components
C. Reduced storage capacity
D. Limited network connectivity
Answer: A

79.What are email spam filters?
A. Filters used to block sensitive information sent via email
B. Filters used to block all incoming email
C. Filters used to block only unsolicited and unwanted email
D. Filters used to block all outgoing email
Answer: C

80.What is end-to-end encryption?
A. A method for optimizing website performance
B. A software development process
C. A type of encryption that protects data as it travels between two endpoints
D. A technique for compressing files
Answer: C

81.Which of the following is a security implication of shared access to data in the cloud?
A. Increased risk of unauthorized access to data
B. Improved data security
C. Improved data accessibility
D. Decreased risk of data loss
Answer: A

82.Which of the following fields in an X.509 certificate identifies the domain name of a website?
A. Issuer
B. Subject
C. Validity
D. subjectAltName
Answer: D

83.Which of the following concepts is related to the process of verifying a user's identity?
A. Authorization
B. Digital identity
C. Authentication
D. Accounting
Answer: C

84.What is information classification?
A. The process of deleting information
B. The process of encrypting information
C. The process of categorizing information based on its sensitivity
D. The process of sharing information with others
Answer: C

85.Which protocol provides secure communication over the Internet by encrypting data in transit?
A. SMTP
B. FTP
C. HTTP
D. HTTPS
Answer: D

KILLTEST

20% de descuento en todos los productos

Obtenga la versión completa de las preguntas del examen

020-100

Killtest.es